

MCAST

Computer Security Laboratory Project

Project #3—System Intrusion Monitoring

Network and system intrusion monitoring is a very important activity that system administrators have to constantly perform. The objective of this project is to understand network and system intrusion monitoring in a Windows operating system. You are required to install and utilize the MS Log Parser toolkit for system and security event monitoring.

Goal: Produce a plan to perform network and system intrusion monitoring

Task 1: Read the documentation of Windows Event logs. Enable log and audit monitoring.

Task 2: Read the documentation on MS Log Parser toolkit

Task 3: Install the MS Log Parser toolkit

Task 4: Implement MS Log Parser scripts for network and system intrusion monitoring.

Assessment and Grading Criteria:

Task 1: (15%)

- **What are event logs?**
- **Describe the process of enabling an event audit.**
- **Describe at least 4 types of Windows events.**
- **Describe at least 4 event IDs that may indicate a system attack.**

Task 2: (10%)

- **What is the MS Log Parser toolkit? Describe its main purpose.**
- **Describe at least five (5) types of input format.**
- **Describe at least five (5) types of output format.**

Task 3: (10%)

Successful installation of the MS Log Parser Toolkit

Task 4: (65%)

- **Completion of the following subtasks:**

1. Use the MS Log Parser to view and archive Event Logs. Describe at least four types of events found in the logs.
2. Use the MS Log Parser to generate a report covering the following events: logon failure, audit failure, and user creation.
3. Archive the event logs of DD/MM/YYYY* and produce a report that shows the event failures that happened during that date.
4. Load the archived event logs of DD/MM/YYYY*, save it into a CSV format, and load it into an Excel spreadsheet.
5. Use the MS Log Parser to display a pie-chart that depicts the frequency distribution of user logins.

* Exact date to be specified during class time.